**CHỮ KÍ SỐ PEDERSEN (CHỮ KÝ SỐ FAIL-STOP)**

Nguyễn Thị Hồng

*Lớp cao học K22 – chuyên ngành Khoa học máy tính*

*Khoa Công nghệ thông tin - Trường đại học Sư Phạm Hà Nội*

1. **Sơ đồ chữ ký số Fail-Stop**

Chữ ký số Fail-Stop cung cấp một khả năng an toàn cao để chống lại những kẻ tấn công mạnh có thể giả mạo chữ ký nghĩa là có khả năng chứng minh được chữ ký đó có phải là giả mạo hay không.

Sơ đồ chữ ký Fail-Stop được đưa ra bởi Van Heyst và Pedersen vào năm 1992. Hệ thống gồm thuật toán kí, thuật toán xác minh và thuật toán chứng minh giả mạo. Sau đây là sơ đồ mô tả thuật toán ký, xác minh của Van Heyst và Pedersen:

Cho p=2q+1 là số nguyên tố sao cho q là số nguyên tố và bài toán logarit rời rạc trong Zp là khó giải. Cho α ∈Z\*p là phần tử bậc q. Giả sử, 1≤ a0 ≤ q-1 và định nghĩa $β=α^{a\_{0}} (mod p)$. Các giá trị α, β, p, q, a0 đều do người có thẩm quyền lựa chọn (người đáng tin cậy). Các số p, q, α, β là công khai và cố định còn a0 được giữ bí mật.



1. **Một số tính chất**

***Định nghĩa:*** hai khóa (γ1, γ2, a1, a2, b1, b2) và (γ1’, γ2’, a1’, a2’, b1’, b2’) là tương đương nếu γ1 = γ1’ và γ2 = γ2’.

***Bổ đề 1:*** giả sử K và K’ là các khóa tương đương và giả sử rằng VerK (x,y) = đúng. Khi đó VerK’ (x,y) = đúng.

*Chứng minh:*

Giả sử K=(γ1, γ2, a1, a2, b1, b2) và K’=(γ1’, γ2’, a1’, a2’, b1’, b2’). Trong đó:



Giả sử, x được ký bằng khóa K được chữ ký y=( γ1, γ2) trong đó:



Bây giờ cần xác minh y bằng cách dung K’:



Như vậy y đã được xác minh bằng K’.

***Bổ đề 2:*** Giả sử K là khóa và y = SigK(x). Khi đó tồn tại đúng q khóa K’ tương đương với K sao cho y= SigK’(x).

*Chứng minh:* Giả sử γ1, γ2 là các thành phần công khai của K. Ta cần xác định bộ 4 (a1, a2, b1, b2) sao cho các đồng dư thức sau được thỏa mãn:



Tồn tại duy nhất các số mũ c1, c2, a0 sao cho:



Như vậy, điều kiện cần và đủ để hệ các đồng dư thức sau đây thỏa mãn:



Hệ đồng dư thức này có thể viết dưới dạng ma trận trong Zq như sau:



Có thể thấy ma trận trên có hạng 3. Hệ phương trình này có ít nhất một nghiệm nhận được bằng cách dung khóa K. Vì hạng của ma trận hệ số bằng 3 nên chiều của không gian nhiệm là 4-3=1 và có chính xác q nghiệm.

Tương tự ta cũng có thể chứng minh được kết quả sau:

***Bổ đề 3:*** giả sử K là khóa, y=Sigk(x) và VerK’(x’,y’)= đúng với x khác x’. Khi đó tồn tại ít nhất một khóa K’ tương đương với K sao cho: y=SigK’(x) và y’=SigK’(x’)

***Định lý:*** Nếu cho trước SigK(x) và x khác x’. Eve có thể tính SigK(x’) với xác suất là 1/q.

*Chứng minh:*

Chú ý, định lý này không phụ thuộc vào khả năng tính toán của Eve, độ an toàn quy định đạt được vì Eve không thể nói về q khóa có thể Bob đang dung. Vì vậy độ an toàn ở đây là vô điều kiện.

Khi cho chữ ký y trên bức điện x, Eve không thể tính ra được chữ ký y’ của Bob trên bức điện x’ khác. Điều này cũng có thể hiểu rằng Eve có thể tính được chữ ký giả mạo y’’= SigK(x’). Tuy nhiên nếu đưa cho Bob một chữ ký giả mạo hợp lệ, anh ta có thể tạo ra bằng chứng về sự giả mạo với xác suất là 1-1/q. Bằng chứng giả mạo chính là giá trị a0=logαβ (chỉ có người thẩm quyền trung tâm biết).

Giả sử Bob đang có cặp (x’, y’’) sao cho Ver(x’, y’’)= đúng và y’’≠ SigK(x’). Có nghĩa là:

$γ\_{1}γ\_{2}^{x'}≡α^{y^{''}\_{1}}β^{y^{''}\_{2}}(mod p)$ với y’’=(y’’1, y’’2)

Lúc này Bob có thể tính chữ ký của mình trên x’ là y’=(y’1, y’2). Khi đó:

$γ\_{1}γ\_{2}^{x'}≡α^{y^{'}\_{1}}β^{y^{'}\_{2}}(mod p)$.

Do đó:$ $

$$α^{y^{''}\_{1}}β^{y^{''}\_{2}}≡α^{y^{'}\_{1}}β^{y^{'}\_{2}}(mod p)$$

Nếu viết $β=α^{a\_{0}}$, ta có:



Hay



Hoặc



Ta thấy y’2 $\overbar{\ne }$y’’2 (mod q) vì y’ là giả mạo. Do đó, (y’2-y’’2)-1 mod q tồn tại và a0 = logαβ = (y’’1-y’1)(y’2-y’’2)-1 mod q

Tất nhiên ta giả thiết Bob không thể tự tính được logarit rời rạc logαβ. Đây là giả thiết về mặt tính toán.

Sơ đồ chữ kí là một lần vì khóa K của Bob có thể tính dễ dàng nếu hai bức điện đều sử dụng cùng một khóa K để kí.

1. **Ví dụ**
* Cho p=3467=2×1733+1.
* Phần tử α = 4 là phần tử bậc 1733 trong Z\*3467.
* Giả sử rằng a0=1567, suy ra β=41567 mod 3467 = 514 (giả sử rằng Bob biết giá trị của α và β song khong biết a0).
* Giả sử Bob lập khóa bằng cách dung a1=888, a2=1024, b1=786, b2=999.

Vậy: γ1=48885141024 mod 3467=3405 và γ2=4786514999 mod 3427 = 2281.

Với bức điện 3383, chữ ký trên bức điện được tính như sau:

y1=888+3383×786 mod 1733=1504

y2=1024+3383×999 mod 1733=1291

Lúc này, giả sử Bob nhận được chữ kí giả mạo (882, 55) trên bức điện 3383. Đây là chữ kí hợp lệ vì thỏa mãn điều kiện xác minh:

3405×22813383≡2282( mod 3467)

Và 482251455≡2282(mod 3467)

Để chứng minh đây là sự giả mạo, ta tính logarit rời rạc bí mật:

a0=(822-1504)(1291-55)mod 1733 =1567

Đây chính là bằng chứng về sự giả mạo!